Addressing Today's Mobile Threats

*Today, mobile devices are prime targets for cybercriminals because they contain more and more sensitive employee, constituent and operational data. **Jim Kovach**, vice president for public sector at Zimperium, explains why signature-based threat detection is obsolete and device attestation is in.*

How has the risk landscape changed with the introduction of mobile devices and mobile applications into government enterprises?

With the shift toward remote work, everybody is using multiple devices. It's not just the laptop anymore. A lot of folks are working from their personal devices and their government-issued device. More devices than ever are connecting to government infrastructure, which means the overall threat landscape has dramatically expanded over just the last few years. We've seen a skyrocketing number of phishing attacks. People get phished through their text SMS channel daily. We've also seen a dramatic rise in zero-day attacks. One-third of all zero-day attacks are now targeted at iOS and Android devices, and one-fifth of mobile endpoints worldwide have encountered malicious applications.

What challenges do state and local governments encounter in securing mobile devices and applications?

These organizations have been underfunded for many years, so they haven't been able to invest in keeping their defensive arsenals up to date. They're not equipped to deal with the growing threat landscape and modern-day attacks such as ransomware. Essentially, they're attempting to address today's threats with yesterday's technology. Virtual private networks and mobile device management have specific purposes and were never designed to do threat detection, be it phishing attacks, rogue Wi-Fi attacks or device threats.

How can organizations close the Zero-Trust gap in their mobile strategies?

A lot of Zero-Trust conversations today revolve around validating identity and making sure that a person is who they purport to be. However, if their device has a malicious payload when they're granted network access, then all we've really done is identify that they were the source of the attack. We believe that when you validate the person's identity, you must simultaneously do device attestation to validate the integrity of their device. Only then should the person be granted access to that particular resource or infrastructure. You can't say you have Zero Trust if you haven't attested the device. The two go hand-in-hand.

How can organizations strengthen mobile application security without disrupting existing programs?

Again, you need to modernize to address today's threats. If you're performing mobile application development, keep in mind that it requires a specific tool set, separate and distinct from traditional web application development. In addition, it's important to protect against zero-day attacks, which are increasing. Signature-based threat detection technology is obsolete. With the advent of machine learning and AI, there are better solutions for identifying and addressing threats that you've never seen before.

How can organizations better secure mobile devices themselves?

It's important to implement a mobile threat defense solution that integrates with the organization's existing IT ecosystem or "tech stack." When organizations evaluate solutions, an important criteria should be integration with identity management, device management, office productivity programs and other parts of the organization's ecosystem.

Where should organizations start on an enterprise mobile security program?

A number of resources will help organizations get a good understanding of the ecosystem. The National Institute of Standards and Technology (NIST) produces a wide variety of reference architectures and practice guides, where they have performed and documented real-world implementations and constructed best practices. I highly recommend NIST SP 800-124 rev 2, which provides comprehensive guidelines for managing the security of mobile devices. The Cybersecurity and Infrastructure Security Agency (CISA) has an entire section of mobile resources and content for organizations that want to get started. Finally, the Advanced Technology Academic Research Center (ATARC) has a Zero-Trust lab series that includes best practices, reference architectures and actual demonstrations. Apart from that, I'd encourage organizations to take advantage of current federal funding opportunities where possible.

Learn more at **Carah.io/2022-GovTech-July-Zimperium**

ZIMPERIUM®

Mobile Device and Application Security for Government & Federal Agencies

Learn more at zimperium.com/fed